

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
SEATTLE DIVISION

MARK GLINOCA, JAMES SMITH, JENNIFER STEPHENS, CHARLES POPP, RUDOLPH WINN, STEPHANIE MILLER, KARLA WILLIAMS, and CHRIS JARVIS on behalf of themselves and a class of all others similarly situated,

Plaintiffs,

v.

T-MOBILE USA, INC.,

Defendant.

Civil Action No.

**COMPLAINT and
DEMAND FOR JURY TRIAL**

Plaintiffs Mark Glinoga, James Smith, Jennifer Stephens, Charles Popp, Rudolph Winn, Stephanie Miller, Karla Williams, and Chris Jarvis (collectively, “Plaintiffs”) individually and on behalf of a class of persons similarly situated (the “Class”) bring this class action against Defendant T-Mobile USA, Inc. (“T-Mobile” or “Defendant”) seeking equitable relief and damages as set forth below.

INTRODUCTION

1. Plaintiffs bring this class action against T-Mobile relating to its failure to protect the confidential information of millions of current, former, and prospective T-Mobile customers.

2. On August 15, 2021, Vice’s Motherboard first reported that T-Mobile suffered a massive data breach. According to the article, a hacker posted to an online forum claiming to have obtained “data related to over 100 million people,” which “came from T-Mobile servers.”¹ The hacker was attempting to sell that data.

3. On August 17, 2021, T-Mobile confirmed that T-Mobile’s systems were subject to a cyberattack that compromised data of millions of their current, former, and prospective customers (the “Data Breach”). Specifically, T-Mobile confirmed that the data accessed included customers’ first and last names, dates of birth, Social Security numbers, and driver’s license/ID information (the “Private Information”).²

4. T-Mobile’s preliminary analysis revealed that approximately 7.8 million current and over 40 million former or prospective customers’ data were contained in the stolen files.³

5. On August 20, 2021, T-Mobile announced that more accounts than originally reported were subject to the Data Breach. Specifically, T-Mobile revealed that another 5.3 million current postpaid customer accounts were accessed, and an additional 667,000 former T-Mobile customer accounts were accessed.⁴ T-Mobile also revealed that in addition to phone numbers, IMEI and IMSI information, the typical identifier numbers associated with a mobile phone, were also compromised.⁵

¹ Joseph Cox, *T-Mobile Investigating Claims of Massive Customer Data Breach*, VICE (Aug. 15, 2021) <https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million> (last visited August 31, 2021).

² Press Release, T-Mobile, T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack (Aug. 17, 2021) <https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation> (last visited on Sept. 10, 2021).

³ *Id.*

⁴ *Id.*

⁵ *Id.*

1 11. Plaintiff James Smith is a resident of the State of Florida. Plaintiff Smith is a
2 current customer of T-Mobile. As part of Plaintiff Smith's relationship with T-Mobile, he
3 provided and entrusted T-Mobile with confidential and sensitive personal information. For
4 example, T-Mobile maintained Plaintiff Smith's name, address, date of birth, and Social Security
5 number, among other things, in one of its databases.

6 12. Plaintiff Smith's personal and confidential information was compromised as a
7 result of the Data Breach.

8 13. T-Mobile verified that Plaintiff Smith's information had been compromised. T-
9 Mobile notified Plaintiff Smith on the T-Mobile app stating that it "has determined that
10 unauthorized access" to his data had occurred.

11 14. Plaintiff Smith would not have entrusted his confidential and sensitive personal
12 information to T-Mobile had he known that T-Mobile failed to maintain adequate data
13 security. As a result of the Data Breach, Plaintiff Smith has been and will continue to be at
14 heightened risk for fraud and identity theft for years to come.

15 15. Plaintiff Jennifer Stephens is a resident of the State of Idaho. Plaintiff Stephens
16 is a current customer of T-Mobile. As part of Plaintiff Stephens' relationship with T-Mobile, she
17 provided and entrusted T-Mobile with confidential and sensitive personal information. For
18 example, T-Mobile maintained Plaintiff Stephens' name, address, date of birth, and Social
19 Security number, among other things, in one of its databases.

20 16. Plaintiff Stephens' personal and confidential information was compromised as a
21 result of the Data Breach.

1 17. T-Mobile verified that Plaintiff Stephens' information had been
2 compromised. On August 19, 2021, T-Mobile texted Plaintiff Stephens stating that it "has
3 determined that unauthorized access" to her data had occurred.

4 18. Plaintiff Stephens would not have entrusted her confidential and sensitive
5 personal information to T-Mobile had she known that T-Mobile failed to maintain adequate data
6 security. As a result of the Data Breach, Plaintiff Stephens has been and will continue to be at
7 heightened risk for fraud and identity theft for years to come.

8 19. Plaintiff Charles Popp is a resident of the State of Illinois. Plaintiff Popp is a
9 current customer of T-Mobile. As part of Plaintiff Popp's relationship with T-Mobile,
10 he provided and entrusted T-Mobile with confidential and sensitive personal information. For
11 example, T-Mobile maintained Plaintiff Popp's name, address, date of birth, and Social Security
12 number, among other things, in one of its databases.

13 20. Plaintiff Popp's personal and confidential information was compromised as a
14 result of the Data Breach.

15 21. T-Mobile verified that Plaintiff Popp's information had been
16 compromised. On August 19, 2021, T-Mobile texted Plaintiff Popp stating that it "has
17 determined that unauthorized access" to his data had occurred.

18 22. Plaintiff Popp would not have entrusted his confidential and sensitive personal
19 information to T-Mobile had he known that T-Mobile failed to maintain adequate data
20 security. As a result of the Data Breach, Plaintiff Popp has been and will continue to be at
21 heightened risk for fraud and identity theft for years to come.

22 23. Plaintiff Rudolph Winn is a resident of the State of New York. Plaintiff Winn is
23 a current customer of T-Mobile. As part of Plaintiff Winn's relationship with T-Mobile,
24

1 he provided and entrusted T-Mobile with confidential and sensitive personal information. For
2 example, T-Mobile maintained Plaintiff Winn's name, address, date of birth, and Social Security
3 number, among other things, in one of its databases.

4 24. Plaintiff Winn's personal and confidential information was compromised as a
5 result of the Data Breach.

6 25. T-Mobile verified that Plaintiff Winn's information had been compromised. On
7 August 19, 2021, T-Mobile texted Plaintiff Winn stating that it "has determined that
8 unauthorized access" to his data had occurred.

9 26. Plaintiff Winn would not have entrusted his confidential and sensitive personal
10 information to T-Mobile had he known that T-Mobile failed to maintain adequate data
11 security. As a result of the Data Breach, Plaintiff Winn has been and will continue to be at
12 heightened risk for fraud and identity theft for years to come.

13 27. Plaintiff Stephanie Miller is a resident of the State of North Carolina. Plaintiff
14 Miller is a current customer of T-Mobile. As part of Plaintiff Miller's relationship with T-
15 Mobile, she provided and entrusted T-Mobile with confidential and sensitive personal
16 information. For example, T-Mobile maintained Plaintiff Miller's name, address, date of birth,
17 and Social Security number, among other things, in one of its databases.

18 28. Plaintiff Miller's personal and confidential information was compromised as a
19 result of the Data Breach.

20 29. T-Mobile verified that Plaintiff Miller's information had been compromised. On
21 August 16, 2021, T-Mobile texted Plaintiff Miller stating that it "has determined that
22 unauthorized access" to her data had occurred.

1 30. Plaintiff Miller would not have entrusted her confidential and sensitive personal
2 information to T-Mobile had she known that T-Mobile failed to maintain adequate data
3 security. As a result of the Data Breach, Plaintiff Miller has been and will continue to be at
4 heightened risk for fraud and identity theft for years to come.

5 31. Plaintiff Karla Williams is a resident of the State of Texas. Plaintiff Williams is
6 a current customer of T-Mobile. As part of Plaintiff Williams' relationship with T-Mobile, she
7 provided and entrusted T-Mobile with confidential and sensitive personal information. For
8 example, T-Mobile maintained Plaintiff William's name, address, date of birth, and Social
9 Security number, among other things, in one of its databases.

10 32. Plaintiff Williams' personal and confidential information was compromised as a
11 result of the Data Breach.

12 33. T-Mobile verified that Plaintiff Williams' information had been
13 compromised. On August 19, 2021, T-Mobile texted Plaintiff Williams stating that it "has
14 determined that unauthorized access" to her data had occurred.

15 34. Plaintiff Williams would not have entrusted her confidential and sensitive
16 personal information to T-Mobile had she known that T-Mobile failed to maintain adequate data
17 security. As a result of the Data Breach, Plaintiff Williams has been and will continue to be at
18 heightened risk for fraud and identity theft for years to come.

19 35. Plaintiff Chris Jarvis is a resident of the State of West Virginia. Plaintiff Jarvis is
20 a current customer of T-Mobile. As part of Plaintiff Jarvis' relationship with T-Mobile,
21 he provided and entrusted T-Mobile with confidential and sensitive personal information. For
22 example, T-Mobile maintained Plaintiff Jarvis' name, address, date of birth, and Social Security
23 number, among other things, in one of its databases.

36. Plaintiff Jarvis's personal and confidential information was compromised as a result of the Data Breach.

37. T-Mobile verified that Plaintiff Jarvis's information had been compromised. During the week of August 16, 2021, T-Mobile notified Plaintiff Jarvis via email and on the T-Mobile app stating that it "has determined that unauthorized access" to his data had occurred.

38. Plaintiff Jarvis would not have entrusted his confidential and sensitive personal information to T-Mobile had he known that T-Mobile failed to maintain adequate data security. As a result of the Data Breach, Plaintiff Jarvis has been and will continue to be at heightened risk for fraud and identity theft for years to come.

39. Defendant T-Mobile USA, Inc. is a Delaware corporation with its principal place of business located at 12920 SE 38th Street, Bellevue, Washington, 98006. T-Mobile is an American wireless network operator and provides wireless voice and data services in the United States. T-Mobile is the second largest wireless carrier in the United States.

JURISDICTION AND VENUE

40. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 (“CAFA”) because at least one member of the Class, as defined below, is a citizen of a different state than T-Mobile, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds \$5,000,000, exclusive of interest and costs. This Court also has diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(a).

41. The Court has personal jurisdiction over this action because T-Mobile maintains its principal place of business in this District, has sufficient minimum contacts with this District,

1 and has purposefully availed itself of the privilege of doing business in this District such that it
2 could reasonably foresee litigation being brought in this District.

3 42. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because T-Mobile's
4 principal place of business is located in this District and a substantial part of the events or
5 omissions giving rise to the claims occurred in, was directed to, and/or emanated from this
6 District.

7 **FACTUAL ALLEGATIONS**

8 **The Data Breach**

9 43. T-Mobile is the second-largest U.S. mobile carrier with roughly 90 million
10 cellphones connecting to its networks.

11 44. On August 15, 2021, *Vice's Motherboard* reported that T-Mobile suffered a
12 massive data breach and hackers claimed to have stolen personal information for over 100 million
13 individuals from T-Mobile.

14 45. According to the article, a hacker posted to an online forum claiming to have
15 obtained "data related to over 100 million people," which "came from T-Mobile servers."⁶ The
16 hacker was attempting to sell that data. According to the article, the hacker was asking for 6
17 Bitcoin, or around \$270,000, for a subset of the data containing 30 million social security
18 numbers and driver licenses.⁷

19 46. On August 16, 2021, T-Mobile released a "Cybersecurity Incident Update"
20 indicating that "[w]e have determined that unauthorized access to some T-Mobile data occurred,
21

22 ⁶ Joseph Cox, *T-Mobile Investigating Claims of Massive Customer Data Breach*, VICE (Aug. 15, 2021)
23 <https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million> (last visited
24 August 31, 2021).

⁷ *Id.*

1 however we have not yet determined that there is any personal customer data involved. We are
 2 confident that the entry point used to gain access has been closed, and we are continuing our deep
 3 technical review of the situation across our systems to identify the nature of any data that was
 4 illegally accessed.”⁸

5 47. On August 17, 2021, T-Mobile released an update confirming that “[w]hile our
 6 investigation is still underway and we continue to learn additional details, we have now been able
 7 to confirm that the data stolen from our systems did include some personal information.”⁹ T-
 8 Mobile revealed that “[s]ome of the data accessed did include customers’ first and last names,
 9 date of birth, SSN, and driver’s license/ID information for a subset of current and former postpay
 10 customers and prospective T-Mobile customers.”¹⁰

11 48. T-Mobile revealed that “approximately 7.8 million current T-Mobile postpaid
 12 customer accounts’ information appears to be contained in the stolen files, as well as just over
 13 40 million records of former or prospective customers who had previously applied for credit with
 14 T-Mobile.”

15 49. In or around August 19, 2021, T-Mobile began notifying its customers via text
 16 message, email, or on the T-Mobile app, that a data breach had occurred and that their personal
 17 data had been stolen by certain unauthorized individuals.

18 50. On August 20, 2021, T-Mobile announced that more accounts than originally
 19 reported were subject to the Data Breach. Specifically, T-Mobile revealed that another 5.3
 20

21 ⁸ Press Release, T-Mobile, T-Mobile Cybersecurity Incident Update (Aug. 16, 2021) [https://www.t-](https://www.t-mobile.com/news/network/cybersecurity-incident-update-august-2021)
 22 [mobile.com/news/network/cybersecurity-incident-update-august-2021](https://www.t-mobile.com/news/network/cybersecurity-incident-update-august-2021) (last visited Sept. 10, 2021).

23 ⁹ Press Release, T-Mobile, T-Mobile Shares Updated Information Regarding Ongoing Investigation into
 24 [Cyberattack](https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation) (Aug. 17, 2021) [https://www.t-mobile.com/news/network/additional-information-regarding-2021-](https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation)
[cyberattack-investigation](https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation) (last visited on Sept. 10, 2021).

¹⁰ *Id.*

1 million current postpaid customer accounts were accessed, and an additional 667,000 former T-
 2 Mobile customer accounts were accessed.¹¹ T-Mobile also revealed that in addition to phone
 3 numbers, IMEI and IMSI information, the typical identifier numbers associated with a mobile
 4 phone, were also compromised.¹²

5 51. Numerous online resources confirm that the personal customer information stolen
 6 from T-Mobile is available for sale.¹³

7 **T-Mobile's Lax Security Measures**

8 52. According to reporting by the Wall Street Journal, T-Mobile's security protocols
 9 were weak and offered an easy path for a hacker to access T-Mobile's records. Specifically, the
 10 hacker who is taking responsibility for breaking into T-Mobile's systems said that T-Mobile's
 11 "lax security eased his path into a cache of records with personal details on more than 50 million
 12 people and counting."¹⁴ The hacker stated, "I was panicking because I had access to something
 13 big . . . Their security is awful."¹⁵

14 53. The Wall Street Journal referenced messages by the hacker who says he had
 15 simply scanned T-Mobile's known internet addresses for weak spots using a simple tool available
 16 to the public.¹⁶

19 ¹¹ *Id.*

20 ¹² *Id.*

21 ¹³ See, e.g., *T-Mobile: Hackers Accessed Data on More Than 53 Million People*, PC MAG (Aug. 27, 2021)
<https://www.pcmag.com/news/t-mobile-reportedly-investigates-data-breach-affecting-up-to-100-million> (last
 22 visited Sept. 10, 2021) (reporting that the hacker asked for 6 Bitcoin, which is worth roughly \$276,000, in
 exchange for the SSNs and driver's license information of 30 million people and that the rest of the data is being
 sold privately rather than being made publicly available.)

23 ¹⁴ *T-Mobile Hacker Who Stole Data on 50 Million Customers: 'Their Security Is Awful'*, THE WALL STREET
 JOURNAL, [https://www.wsj.com/articles/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-](https://www.wsj.com/articles/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105#)
[is-awful-11629985105#](https://www.wsj.com/articles/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105#) (last visited on September 10, 2021).

24 ¹⁵ *Id.*

¹⁶ *Id.*

54. This is not the first time T-Mobile's inadequate data security measures were the cause of a data breach. For example, in 2018, hackers accessed personal information for roughly two million T-Mobile customers that included names, addresses, and account numbers, and in 2019, some of T-Mobile's prepaid customers were affected by a breach that also accessed names, addresses, and account numbers.¹⁷ A March 2020 breach exposed certain T-Mobile customers' financial information, Social Security numbers, and other account information.¹⁸ In December 2020, T-Mobile discovered another data breach in which hackers accessed customer proprietary network information and undisclosed call related information for hundreds of thousands of customers.¹⁹ Additionally, in February 2021, T-Mobile notified customers that cyberthieves gained access to customer account information, including full names, addresses, email addresses, account numbers, Social Security numbers, account PINs, account security questions and answers, dates of birth, and plan information.²⁰

55. Several cybersecurity experts said the Data Breach and the previous breaches show that the carrier's defenses need improvement.²¹ Many of the records reported stolen were from prospective clients or former customers.²² Glenn Gerstell, a former general counsel for the

¹⁷ *T-Mobile investigating report of customer data breach that reportedly involves 100 million people*, THE VERGE (Aug. 15, 2021) <https://www.theverge.com/2021/8/15/22626270/t-mobile-investigating-report-customer-data-breach> (last visited on Sept. 10, 2021).

¹⁸ *Id.*

¹⁹ *Second Data Breach in 2020 for T-Mobile Exposed Customer and Call-Related Information of 200,000 Subscribers*, CPO MAGAZINE (Jan. 11, 2021) <https://www.cpomagazine.com/cyber-security/second-data-breach-in-2020-for-t-mobile-exposed-customer-and-call-related-information-of-200000-subscribers/> (last visited on Sept. 10, 2021).

²⁰ *T-Mobile discloses data breach after SIM swapping attacks*, BLEEPING COMPUTER (Feb. 26, 2021) <https://www.bleepingcomputer.com/news/security/t-mobile-discloses-data-breach-after-sim-swapping-attacks/> (last visited Sept. 10, 2021).

²¹ *T-Mobile Hacker Who Stole Data on 50 Million Customers: 'Their Security Is Awful'*, THE WALL STREET JOURNAL (Aug. 27, 2021) <https://www.wsj.com/articles/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105#> (last visited Sept. 10, 2021).

²² *Id.*

1 National Security Agency stated, “[t]hat to me does not sound like good data management
2 practices.”²³

3 56. Despite these prior breaches, T-Mobile failed to adopt adequate protective
4 measures to ensure that consumers’ Private Information would not be improperly accessed.

5 **The Data Breach Harmed Customers and Putative Class Members**

6 57. Plaintiffs and Class members suffered actual injury from having their Private
7 Information compromised as a result of the data breach including, but not limited to: (a) damage
8 to and diminution in the value of their Private Information, a form of property that T-Mobile
9 obtained from Plaintiffs and Class members; (b) violation of their privacy rights; (c) imminent
10 and impending injury arising from the increased risk of identity theft and fraud; and (d) time and
11 resources spent mitigating the harm.

12 58. When a hacker is able to access a person’s Private Information, they can use it to
13 commit a whole host of cybercrimes. These cybercrimes are rising at an exponential rate, as
14 shown in the FBI’s Internet Crime Complaint statistics chart below²⁴:

23 *Id.*

24 Internet Crime Report 2021, Federal Bureau of Investigation
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited Sept. 10, 2021).

IC3 Complaint Statistics

Last Five Years

2,211,396 TOTAL COMPLAINTS



\$13.3 Billion TOTAL LOSSES*

(Rounded to the nearest million)

59. To emphasize the large-scale impact of cybercrime, a study released in February 2018 by McAfee and the think tank Center for Strategic and International Studies shows that worldwide, cybercrime costs an estimated \$600 billion USD a year. This increased from \$500 billion USD in 2014. The new estimate amounts to 0.8 percent of global gross domestic product.²⁵

60. Plaintiffs and Class members are at risk for identity theft in its myriad forms, potentially for the remainder of their lives.

61. Identity thieves can use the Private Information to harm Plaintiffs and Class

²⁵ *The Cost of Cybercrime*, INTERNET SOCIETY (Feb. 23, 2018) <https://internetsociety.org/blog/2018/02/the-cost-of-cybercrime/> (last visited on Sept. 10, 2021).

1 members through embarrassment, blackmail, or harassment in person or online, or to commit
2 other types of fraud including, but not limited to, obtaining ID cards or driver's licenses,
3 fraudulently obtaining tax returns and refunds, obtaining government benefits, and/or opening
4 financial accounts.

5 62. In addition to the losses that result when identity thieves fraudulently open
6 accounts or misuse existing accounts, individual victims often suffer indirect financial costs,
7 including the costs incurred in both civil litigation initiated by creditors and in overcoming the
8 many obstacles they face in obtaining or retaining credit.

9 63. In addition to out-of-pocket expenses that can reach thousands of dollars for the
10 victims of new account identity theft, and the emotional toll identity theft can take, some victims
11 have to spend what can be a considerable amount of time to repair the damage caused by the
12 identity thieves. Victims of new account identity theft, for example, must correct fraudulent
13 information in their credit reports and monitor their reports for future inaccuracies, close existing
14 bank accounts and open new ones, and dispute charges with individual creditors.

15 64. The problems associated with identity theft are exacerbated by the fact that many
16 identity thieves will wait years before attempting to use the Private Information they have
17 obtained. Indeed, to protect themselves, Class members will need to remain vigilant against
18 unauthorized data use for years and decades to come.

19 65. Once stolen, the Private Information can be used in several different ways. One
20 of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of
21 the Internet that makes it difficult for authorities to detect the location or owners of a website.
22 The dark web is not indexed by normal search engines such as Google and is only accessible
23 using a Tor browser (or similar tool), which aims to conceal users' identities and online activity.
24

1 The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs,
 2 and personal identifying information. Websites appear and disappear quickly, making it a very
 3 dynamic environment.

4 66. Once someone buys Private Information, it is then used to gain access to different
 5 areas of the victim's digital life, including bank accounts, social media, and credit card details.
 6 During that process, other sensitive data may be harvested from the victim's accounts, as well as
 7 from those belonging to family, friends, and colleagues.

8 67. Further, an individual's Private Information has market value and there are
 9 markets for that Private Information. For example, data collection companies, credit reporting
 10 companies, and companies that engage in targeted advertising are all willing to pay money to
 11 obtain, directly or indirectly, Private Information from individuals. Indeed, many email and
 12 social media service providers require their users to consent to having their information scanned
 13 and recorded for selling that information to advertisers. But, the theft of that Private Information
 14 and unauthorized sale of it on the "dark web" diminishes its legitimate market value.

15 **CLASS ACTION ALLEGATIONS**

16 68. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this
 17 lawsuit on behalf of themselves and the following proposed Nationwide Class, defined as
 18 follows:

19 All current, former, and prospective T-Mobile customers residing in the United
 20 States whose private information was compromised in the Data Breach announced
 by T-Mobile on or about August 16, 2021 (the "Nationwide Class").

21 69. The California Subclass is defined as follows:

22 All current, former, and prospective T-Mobile customers residing in California
 23 whose Private Information was compromised in the Data Breach announced by
 T-Mobile on or about August 16, 2021 (the "California Subclass").

70. The Florida Subclass is defined as follows:

All current, former, and prospective T-Mobile customers residing in Florida whose Private Information was compromised in the Data Breach announced by T-Mobile on or about August 16, 2021 (the “Florida Subclass”).

71. The Idaho Subclass is defined as follows:

All current, former, and prospective T-Mobile customers residing in Idaho whose Private Information was compromised in the Data Breach announced by T-Mobile on or about August 16, 2021 (the “Idaho Subclass”).

72. The Illinois Subclass is defined as follows:

All current, former, and prospective T-Mobile customers residing in Illinois whose Private Information was compromised in the Data Breach announced by T-Mobile on or about August 16, 2021 (the “Illinois Subclass”).

73. The New York Subclass is defined as follows:

All current, former, and prospective T-Mobile customers residing in New York whose Private Information was compromised in the Data Breach announced by T-Mobile on or about August 16, 2021 (the “New York Subclass”).

74. The North Carolina Subclass is defined as follows:

All current, former, and prospective T-Mobile customers residing in North Carolina whose Private Information was compromised in the Data Breach announced by T-Mobile on or about August 16, 2021 (the “North Carolina Subclass”).

75. The Texas Subclass is defined as follows:

All current, former, and prospective T-Mobile customers residing in Texas whose Private Information was compromised in the Data Breach announced by T-Mobile on or about August 16, 2021 (the “Texas Subclass”).

76. The West Virginia Subclass is defined as follows:

All current, former, and prospective T-Mobile customers residing in West Virginia whose Private Information was compromised in the Data Breach announced by T-Mobile on or about August 16, 2021 (the “West Virginia Subclass”).

77. Excluded from the Class are T-Mobile and any entities in which T-Mobile or its

1 subsidiaries or affiliates have a controlling interest; T-Mobile's officers, agents, and employees;
 2 the judicial officers to whom this action is assigned; and any member of the Court's staff and
 3 immediate families.

4 78. **Numerosity:** The members of the Class are so numerous that joinder of all
 5 members would be impracticable. Plaintiffs reasonably believe that the Class includes millions
 6 of individuals. As such, Class members are so numerous that joinder of all members is
 7 impractical. The names and addresses of Class members are identifiable through documents
 8 maintained by T-Mobile.

9 79. **Commonality and Predominance:** This action involves common questions of
 10 law or fact, which predominate over any questions affecting individual Class members,
 11 including:

- 12 a. Whether T-Mobile engaged in the wrongful conduct alleged herein;
- 13 b. Whether T-Mobile's inadequate data security measures were a cause of the Data
 14 Breach;
- 15 c. Whether T-Mobile owed a legal duty to Plaintiffs and the other Class members to
 16 exercise due care in collecting, storing, and safeguarding their Private
 17 Information;
- 18 d. Whether T-Mobile negligently or recklessly breached legal duties owed to
 19 Plaintiffs and the other class members to exercise due care in collecting, storing,
 20 and safeguarding their Private Information;
- 21 e. Whether Plaintiffs and the Class are at an increased risk for identity theft because
 22 of the Data Breach;
- 23
- 24

f. Whether Plaintiffs and the Class have suffered a decrease in the value of their Private Information because of the Data Breach;

g. Whether Plaintiffs and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

h. Whether Plaintiffs and the other Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

80. These issues not only predominate, but they are also matters appropriate for issue certification under Rule 23(c)(4).

81. T-Mobile engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

82. **Typicality:** Plaintiffs' claims are typical of the claims of the other Class members because, among other things, Plaintiffs and the other Class members were injured through the substantially uniform misconduct by T-Mobile. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiffs.

83. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other class members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

84. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against T-Mobile, making it impracticable for class members to individually seek redress for T-Mobile's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

COUNT I **NEGLIGENCE**

(On Behalf of the Nationwide Class or Alternatively State-Specific Subclasses)

85. Plaintiffs re-allege and incorporate by reference herein all the allegations contained above.

86. T-Mobile owed a duty to Plaintiffs and the other Class members to exercise reasonable care in safeguarding and protecting their Private Information that was in its possession from being compromised, lost, stolen, misused, or disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure that Plaintiffs' and the other Class members' Private Information was adequately secured and protected. Defendant further had a duty to implement processes that would detect a breach of their security system in a timely manner.

1 87. By being entrusted by Plaintiffs and the Class to safeguard their Private
2 Information, T-Mobile had a special relationship with Plaintiffs and the Class. Plaintiffs and the
3 Class provided their Private Information to T-Mobile with the understanding that it would take
4 appropriate measures to protect it and would inform Plaintiffs and the Class of any breaches or
5 other security concerns that might call for action by Plaintiffs and the Class. But, T-Mobile did
6 not. T-Mobile knew its data security was inadequate.

7 88. T-Mobile breached the duties owed to Plaintiff and Class Members and thus was
8 negligent. T-Mobile breached these duties by, among other things, failing to: (a) exercise
9 reasonable care and implement adequate security systems, protocols and practices sufficient to
10 protect the Private Information of Plaintiffs and Class Members; (b) detect the breach while it
11 was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose
12 that Plaintiffs' and Class members' Private Information in T-Mobile's possession had been or
13 was reasonably believed to have been, stolen or compromised.

14 89. But for T-Mobile's wrongful and negligent breach of the duties owed to Plaintiffs
15 and the other Class members, their Private Information would not have been compromised,
16 stolen, viewed, and potentially sold by unauthorized persons.

17 90. The injury and harm suffered by Plaintiffs and the other Class members was the
18 reasonably foreseeable result of T-Mobile's failure to exercise reasonable care in safeguarding
19 and protecting Plaintiffs' and the other Class members' Private Information. T-Mobile knew or
20 should have known that their systems and technologies for processing and securing Plaintiffs'
21 and the other Class members' Private Information had security vulnerabilities.

22 91. As a result of Defendant's negligence, Plaintiffs and the other Class members
23 have been harmed and have suffered damages including, but not limited to: damages arising from
24

1 identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and
 2 restoration services; increased risk of future identity theft and fraud, and the costs associated
 3 therewith; and time spent monitoring, addressing, and correcting the current and future
 4 consequences of the Data Breach.

5 **COUNT II**

6 **NEGLIGENCE PER SE**

(On Behalf of the Nationwide Class or Alternatively State-Specific Subclasses)

7 92. Plaintiffs re-allege and incorporate by reference herein all the allegations
 8 contained above.

9 93. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits “unfair . . . practices in or
 10 affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice
 11 by T-Mobile of failing to use reasonable measures to protect Plaintiffs’ and Class members’
 12 Private Information. Various FTC publications and orders also form the basis of T-Mobile’s duty.

13 94. T-Mobile violated Section 5 of the FTC Act (and similar state statutes) by failing
 14 to use reasonable measures to protect Plaintiffs’ and Class members’ Private Information and not
 15 complying with industry standards.

16 95. T-Mobile’s conduct was particularly unreasonable given the nature and amount
 17 of Private Information obtained and stored and the foreseeable consequences of a data breach on
 18 T-Mobile’s systems.

19 96. T-Mobile’s violation of Section 5 of the FTC Act (and similar state statutes)
 20 constitutes negligence per se.

21 97. Class members are consumers within the class of persons Section 5 of the FTC
 22 Act (and similar state statutes) were intended to protect.
 23
 24

1 the monies paid to T-Mobile under the implied contracts to fund adequate and reasonable data
2 security practices.

3 104. Plaintiffs and Class members would not have provided and entrusted their Private
4 Information to T-Mobile or would have paid less for T-Mobile's services in the absence of the
5 implied contract or implied terms between them and T-Mobile. The safeguarding of the Private
6 Information of Plaintiffs and Class members was critical to realize the intent of the parties.

7 105. Plaintiffs and Class members fully performed their obligations under the implied
8 contacts with T-Mobile.

9 106. T-Mobile breached its implied contracts with Plaintiffs and Class members to
10 protect their Private Information when it: (1) failed to have security protocols and measures in
11 place to protect that information; and (2) disclosed that information to unauthorized third parties.

12 **COUNT IV**
13 **VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT ("CCPA"), Cal.**
14 **Civ. Code 1798.150**
(On Behalf of the California Subclass)

15 107. Plaintiffs re-allege and incorporate by reference herein all the allegations
16 contained above.

17 108. Plaintiff Glinoga asserts this claim on behalf of the California Subclass.

18 109. T-Mobile collects consumers' personal information as defined in Cal. Civ. Code
19 Sec. 1798.140.

20 110. Defendant violated Sec. 1798.150 of the CCPA by failing to prevent Plaintiff
21 Glinoga's and Class members' Private Information from unauthorized access and exfiltration,
22 theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain
23 reasonable security procedures and practices appropriate to the nature of the information.

24 111. Defendant at all relevant times had a duty to implement and maintain reasonable

1 security procedures and practices to protect Plaintiff's and Class members' Private Information.
 2 As detailed herein, Defendant failed to do so. As a direct and proximate result of Defendant's
 3 acts, Plaintiff Glinoga's and California Subclass members' Private Information, including social
 4 security numbers, phone numbers, names, addresses, unique IMEI numbers, and driver's license
 5 information, was subjected to unauthorized access and exfiltration, theft, or disclosure.

6 112. Plaintiff Glinoga and California Subclass members seek injunctive or other
 7 equitable relief to ensure Defendant hereinafter adequately safeguards customers' Private
 8 Information by implementing reasonable security procedures and practices. Such relief is
 9 particularly important because Defendant continues to hold customers' Private Information,
 10 including Plaintiff Glinoga's and California Subclass members' Private Information. Plaintiff
 11 Glinoga and California Subclass members have an interest in ensuring that their Private
 12 Information is reasonably protected, and Defendant has demonstrated a pattern of failing to
 13 adequately safeguard this information.

14 113. Pursuant to Cal. Civ. Code Sec. 1798.150, on September 8, 2021, Plaintiff mailed
 15 a CCPA notice letter to Defendant, detailing the specific provisions of the CCPA that T-Mobile
 16 violated. If Defendant cannot cure within 30 days, then Plaintiff intends to promptly amend this
 17 Complaint to seek statutory damages as permitted by the CCPA.

18 **COUNT V**
 19 **VIOLATION OF THE UNFAIR COMPETITION LAW, BUSINESS & PROFESSIONS**
 20 **CODE § 17200, *et seq.***
 (On Behalf of the California Subclass)

21 114. Plaintiffs re-allege and incorporate by reference herein all the allegations
 22 contained above.

23 115. Plaintiff Glinoga asserts this claim on behalf of the California Subclass.
 24

1 116. California's Unfair Competition Law, California Business & Professions Code §
2 17200, et seq. (the "UCL") provides that unfair practices include, but are not limited to, "any
3 unlawful, unfair or fraudulent business act[s] or practice[s]."

4 117. Defendant engaged in activities that constitute unlawful, unfair and fraudulent
5 business practices prohibited by the UCL.

6 118. Defendant knew or should have known that its failure to implement and maintain
7 reasonable security procedures and practices to protect Plaintiff Glinoga's and the other
8 California Subclass members' Private Information was unlawful, unfair, and fraudulent.
9 Defendant willfully ignored the clear and present risk of a security breach of their systems and
10 failed to implement and maintain reasonable security measures to prevent, detect, and mitigate
11 the Data Breach. Defendant benefitted from not taking preventative measures and implementing
12 adequate security measures that would have prevented, detected, and mitigated the Data Breach.

13 119. Defendant's conduct is unlawful because it violates the statutes referenced herein,
14 and constitutes negligence and negligence per se.

15 120. Defendant's conduct was unfair because it violates established public policy
16 established by the FTC and California law governing the security and privacy of consumers'
17 personal information. Defendant's conduct is also immoral, unethical, oppressive or
18 unscrupulous and causes injury to consumers that outweighs its benefits. Any benefit to
19 consumers of Defendant's services is outweighed by the harm to consumers of the disclosure of
20 their Private Information. Consumers could not have avoided this harm themselves.

21 121. Plaintiff Glinoga and the other California Subclass members have suffered actual
22 damages including identity theft, improper disclosure of their Private Information, lost value of
23 their Private Information, and lost time and money incurred to mitigate and remediate the effects
24

1 of the Data Breach.

2 122. Plaintiff Glinoga's and the other California Subclass members' injuries were
3 proximately caused by Defendant's violations of the UCL. Defendant acted with reckless
4 indifference toward the rights of others, such that an award of punitive damages is warranted.

5 123. Plaintiff Glinoga and the other California Subclass members are also entitled to
6 injunctive relief in the form of deletion and destruction of data, greater security practices and
7 protocols, and training and compliance with industry standards governing data security.

8 **COUNT VI**
9 **VIOLATION OF CALIFORNIA'S CONSUMERS LEGAL REMEDIES ACT, Cal. Civ.**
10 **Code §§ 1750, *et seq.***
(On Behalf of the California Subclass)

11 124. Plaintiffs re-allege and incorporate by reference herein all the allegations
12 contained above.

13 125. Plaintiff Glinoga asserts this claim on behalf of the California Subclass.

14 126. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA")
15 is a comprehensive statutory scheme that is to be liberally construed to protect consumers against
16 unfair and deceptive business practices in connection with the conduct of businesses providing
17 goods, property or services to consumers primarily for personal, family, or household use.

18 127. T-Mobile is a "person" as defined by Civil Code §§ 1761(c) and 1770 and has
19 provided "services" as defined by Civil Code §§ 1761(b) and 1770.

20 128. Plaintiff Glinoga and the California Subclass are "consumers" as defined by Civil
21 Code §§ 1761(d) and 1770 and have engaged in a "transaction" as defined by Civil Code §§
22 1761(e) and 1770.

23 129. T-Mobile violated the CLRA by way of Civil Code § 1770(a)(5). In particular,
24

1 T-Mobile represented (and continues to represent) that its services have benefits and
 2 characteristics which they do not have – mainly that T-Mobile has adequate data security
 3 practices to ensure that consumers’ Private Information is safe and secure from unauthorized
 4 disclosure.

5 130. T-Mobile is aware that this misrepresentation, which is a significant factor for its
 6 commercial success, is false and misleading.

7 131. Plaintiff Glinoga and Members of the California Subclass seek injunctive or other
 8 equitable relief to ensure that T-Mobile hereafter adequately safeguards Private Information by
 9 implementing reasonable security procedures and practices. This relief is important because T-
 10 Mobile still holds Private Information related to Plaintiff Glinoga and Members of the California
 11 Subclass. Plaintiff Glinoga and California Subclass members have an interest in ensuring that
 12 their Private Information is reasonably protected.

13 132. Pursuant to Cal. Civ. Code § 1782, on September 8, 2021, Plaintiff Glinoga
 14 mailed T-Mobile notice in writing, via U.S. certified mail, return receipt requested, of the
 15 particular violations of Cal. Civ. Code § 1770 of the CLRA and demand that it rectify the actions
 16 described above. If T-Mobile fails to take the actions demanded to rectify their violations of the
 17 CLRA, Plaintiff Glinoga will amend his complaint seek damages and attorneys’ fees as allowed
 18 by the CLRA.

19 **COUNT VII**
 20 **VIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE**
 21 **PRACTICE ACT (“FDUTPA”), Fla. Stat. § 501.201, *et seq.***
 22 **(On Behalf of the Florida Subclass)**

23 133. Plaintiffs re-allege and incorporate by reference herein all the allegations
 24 contained above.

134. Plaintiff James Smith asserts this claim on behalf of the Florida Subclass.

1 135. FDUTPA prohibits “unfair methods of competition, unconscionable acts or
2 practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce.”
3 Fla. Stat. § 501.204.

4 136. T-Mobile engaged in the conduct alleged in this Complaint through transactions
5 in and involving trade and commerce. Mainly, the Data Breach occurred through the use of the
6 internet, an instrumentality of interstate commerce.

7 137. While engaged in trade or commerce, T-Mobile violated the FDUTPA,
8 including, among other things, by: (1) failing to implement and maintain appropriate and
9 reasonable security procedures and practices to safeguard and protect the Private Information of
10 the Florida Subclass; (2) failing to disclose that its computer systems and data security
11 practices were inadequate to safeguard and protect the Private Information of the Florida
12 Subclass; and (3) failing to disclose the data breach in a timely and accurate manner in violation
13 of Fla. Stat. § 501.171.

14 138. T-Mobile knew or should have known that its computer systems and security
15 practices were inadequate to safeguard Plaintiff Smith’s and the Florida Subclass’ Private
16 Information entrusted to it, and that risk of a data breach or theft was likely.

17 139. T-Mobile should have disclosed this information because T-Mobile was in a
18 superior position to know the true facts related to its defective data security.

19 140. T-Mobile’s failures constitute false and misleading representations, which have
20 the capacity, tendency, and effect of deceiving or misleading consumers, including the Florida
21 Subclass members, regarding the security of T-Mobile’s network and aggregation of Private
22 Information.

23 141. These representations upon which consumers, including the Florida Subclass
24

1 Members, relied were material representations and consumers relied on those representations to
2 their detriment.

3 142. T-Mobile's actions constitute unconscionable, deceptive, or unfair acts or
4 practices because, as alleged herein, T-Mobile engaged in immoral, unethical, oppressive, and
5 unscrupulous activities that are and were substantially injurious to T-Mobile's customers,
6 including Florida Subclass members.

7 143. In committing the acts alleged above, T-Mobile engaged in unconscionable,
8 deceptive, and unfair acts and practices by omitting, failing to disclose, or inadequately disclosing
9 to past, current, and future customers, including the Florida Subclass members, that it did not
10 follow industry best practices for the collection, use, and storage of the Private Information.

11 144. As a direct and proximate result of T-Mobile's unlawful practices and acts,
12 Plaintiff Smith and Florida Subclass members have been harmed and have suffered damages
13 including, but not limited to: damages arising from identity theft and fraud; out-of-pocket
14 expenses associated with procuring identity protection and restoration services; increased risk of
15 future identity theft and fraud, and the costs associated therewith; and time spent monitoring,
16 addressing and correcting the current and future consequences of the Data Breach.

17 145. As a direct and proximate result of T-Mobile's unconscionable, unfair, and
18 deceptive acts and omissions, Plaintiff Smith's and Florida Subclass members' Private
19 Information was disclosed to third parties without authorization, causing and will continue to
20 cause Plaintiffs and Florida Subclass members damages. Accordingly, Plaintiff Smith and
21 Florida Subclass Members are entitled to recovery actual damages, an order providing
22 declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted
23 by law.
24

COUNT VIII
VIOLATION OF IDAHO CONSUMER PROTECTION ACT,
Idaho Code §§ 48-601, et seq.
(On Behalf of the Idaho Subclass)

146. Plaintiffs re-allege and incorporate by reference herein all the allegations contained above.

147. Plaintiff Jennifer Stephens asserts this claim on behalf of the Idaho Subclass.

148. T-Mobile is a “person” as defined by Idaho Code § 48-602(1).

149. T-Mobile’s conduct as alleged herein pertained to “goods” and “services” as defined by Idaho Code § 48-602(6) and (7).

150. T-Mobile advertised, offered, or sold goods or services in Idaho and engaged in trade or commerce directly or indirectly affecting the people of Idaho.

151. T-Mobile engaged in unfair and deceptive acts or practices, and unconscionable acts and practices, in the conduct of trade and commerce with respect to the sale and advertisement of goods and services, in violation of Idaho Code §§ 48-603 including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade, if they are of another; and
- c. Advertising goods or services with intent not to sell them as advertised.

152. T-Mobile’s false, misleading, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Stephens’s and Idaho Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified

1 security and privacy risks, and adequately improve security and privacy
2 measures following previous cybersecurity incidents, which was a direct and
3 proximate cause of the Data Breach; and

- 4 c. Failing to comply with common law and statutory duties pertaining to the
5 security and privacy of Plaintiff Stephens's and Idaho Subclass members'
6 Private Information.

7 153. T-Mobile's representations and omissions were material because they were likely
8 to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to
9 protect the confidentiality of consumers' Private Information.

10 154. T-Mobile intended to mislead Plaintiff Stephens and Idaho Subclass members and
11 induce them to rely on its misrepresentations and omissions. T-Mobile knew its representations
12 and omissions were false.

13 155. T-Mobile acted intentionally, knowingly, and maliciously to violate Idaho's
14 Consumer Protection Act, and recklessly disregarded Plaintiff Stephens' and Idaho Subclass
15 members' rights. T-Mobile's numerous past data breaches put it on notice that its security and
16 privacy protections were inadequate.

17 156. As a direct and proximate result of T-Mobile's unfair, deceptive, and
18 unconscionable conduct, Plaintiff Stephens and Idaho Subclass members have been harmed and
19 have suffered damages including, but not limited to: damages arising from identity theft and
20 fraud; out-of-pocket expenses associated with procuring identity protection and restoration
21 services; increased risk of future identity theft and fraud, and the costs associated therewith; and
22 time spent monitoring, addressing and correcting the current and future consequences of the Data
23 Breach.

157. Plaintiff Stephens and Idaho Subclass members seek all monetary and nonmonetary relief allowed by law, including damages, punitive damages, injunctive relief, costs, and attorneys' fees.

COUNT IX
VIOLATION OF THE ILLINOIS' CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 505/1, et seq. (the "ICFA")
 (On Behalf of the Illinois Subclass)

158. Plaintiffs re-allege and incorporate by reference herein all the allegations contained above.

159. Plaintiff Charles Popp asserts this claim on behalf of the Illinois Subclass.

160. Plaintiff Popp and the Illinois Subclass are "consumers" as that term is defined in 815 Ill. Comp. Stat. § 505/1(e).

161. Plaintiff Popp, the Illinois Subclass, and T-Mobile are "persons" as that term is defined in 815 Ill. Comp. Stat. § 505/1(c).

162. T-Mobile is engaged in "trade" or "commerce," including provision of services, as those terms are defined under 815 Ill. Comp. Stat. § 505/1(f).

163. T-Mobile engages in the "sale" of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

164. T-Mobile engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the ICFA) in violation of the ICFA, including but not limited to failing to maintain sufficient security to keep Plaintiff Popp's and the Illinois Subclass' Private Information from being hacked and stolen.

165. In addition, T-Mobile's failure to disclose that its computer systems were not well-protected and that Plaintiff Popp's and the Illinois Subclass' Private Information was

1 vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts
2 or practices because T-Mobile knew such facts would (a) be unknown to and not easily
3 discoverable by Plaintiff Popp and the Illinois Subclass; and (b) defeat Plaintiff Popp and the
4 Illinois Subclass' ordinary, foreseeable and reasonable expectations concerning the security of
5 their Private Information on T-Mobile servers.

6 166. T-Mobile intended that Plaintiff Popp and the Illinois Subclass rely on its
7 deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression,
8 and omission of material facts, in connection with T-Mobile's offering of goods and services and
9 incorporating Plaintiff Popp's and the Illinois Subclass' Private Information on its servers, in
10 violation of the ICFA.

11 167. T-Mobile also engaged in unfair acts and practices by failing to maintain the
12 privacy and security of Plaintiff Popp's and the Illinois Subclass' Private Information, in
13 violation of duties imposed by and public policies reflected in applicable federal and state laws,
14 resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws
15 including the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

16 168. T-Mobile's wrongful practices occurred in the course of trade or commerce.

17 169. T-Mobile's wrongful practices were and are injurious to the public interest
18 because those practices were part of a generalized course of conduct on the part of T-Mobile that
19 applied to Plaintiff Popp and all Illinois Subclass members and were repeated continuously
20 before and after T-Mobile obtained sensitive Private Information from Plaintiff Popp and the
21 Illinois Subclass. Plaintiff Popp and the Illinois Subclass were adversely affected by T-Mobile's
22 conduct and the public was and is at risk as a result thereof.

23 170. As a result of T-Mobile's wrongful conduct, Plaintiff Popp and the Illinois
24

Subclass were injured in that they never would have allowed their Private Information – the value over which Plaintiff Popp and the Illinois Subclass no longer have control – to be provided to T-Mobile if they had been told or knew that T-Mobile failed to maintain sufficient security to keep such data from being breached.

171. As a direct and proximate result of T-Mobile’s unconscionable, unfair, and deceptive acts and omissions, Plaintiff Popp’s and Illinois Subclass members’ Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff Popp and Illinois Subclass members damages. Accordingly, Plaintiff Popp and Illinois Subclass members are entitled to recovery of actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys’ fees and costs, to the extent permitted by law.

COUNT X
VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW (“GBL”) § 349
 (On Behalf of the New York Subclass)

172. Plaintiffs re-allege and incorporate by reference herein all the allegations contained above.

173. Plaintiff Rudolph Winn asserts this claim on behalf of the New York Subclass.

174. T-Mobile engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of New York’s GBL § 349(a), including but not limited to the following:

- a. T-Mobile misrepresented material facts to Plaintiff Winn and the New York Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard New York Subclass members’ Private Information from unauthorized disclosure, release, data breaches, and theft;

1 b. T-Mobile misrepresented material facts to Plaintiffs Winn and the New York
2 Subclass by representing that it did and would comply with the requirements of
3 federal and state laws pertaining to the privacy and security of Plaintiff Winn's and
4 the New York Subclass' Private Information;

5 c. T-Mobile omitted, suppressed, and concealed material facts of the inadequacy of
6 its privacy and security protections for Plaintiff Winn's and the New York Subclass'
7 Private Information;

8 d. T-Mobile engaged in deceptive, unfair, and unlawful trade acts or practices by
9 failing to maintain the privacy and security of Plaintiff Winn's and New York
10 Subclass members' Private Information, in violation of the duties imposed by and
11 public policies reflected in applicable federal and state laws, resulting in the data
12 breach. These unfair acts and practices violated duties imposed by laws including the
13 Federal Trade Commission Act, 15 U.S.C. § 45;

14 e. T-Mobile engaged in deceptive, unfair, and unlawful trade acts or practices by
15 failing to disclose the data breach to the New York Subclass in a timely and accurate
16 manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2). T-Mobile
17 knew or should have known that its computer systems and data security practices
18 were inadequate to safeguard the New York Subclass Members' Private Information
19 entrusted to it, and that risk of a data breach or theft was highly likely.

20 175. T-Mobile should have disclosed this information because it was in a superior
21 position to know the true facts related to the defective data security.

22 176. T-Mobile's failure constitutes false and misleading representations, which have
23 the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff
24

1 Winn and New York Subclass members) regarding the security of T-Mobile's network and
2 aggregation of Private Information.

3 177. These representations upon which consumers, including the New York Subclass
4 members, relied were material representations and consumers relied on those representations to
5 their detriment.

6 178. T-Mobile's conduct is unconscionable, deceptive, and unfair, as it is likely to, and
7 did, mislead consumers acting reasonably under the circumstances.

8 179. As a direct and proximate result of T-Mobile's unconscionable, unfair, and
9 deceptive acts and omissions, Plaintiff Winn's and New York Subclass members' Private
10 Information was disclosed to third parties without authorization, causing and will continue to
11 cause Plaintiff Winn and New York Subclass members damages.

12 180. Plaintiff Winn and New York Subclass members seek relief under N.Y. Gen. Bus.
13 Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages,
14 injunctive relief, and/or attorney's fees and costs.

15 **COUNT XI**
16 **VIOLATION OF NORTH CAROLINA UNFAIR TRADE PRACTICES ACT,**
17 **N.C. Gen. Stat. Ann. §§ 75-1.1, *et seq.***
(On Behalf of the North Carolina Subclass)

18 181. Plaintiffs re-allege and incorporate by reference herein all the allegations
19 contained above.

20 182. Plaintiff Stephanie Miller asserts this claim on behalf of the North Carolina
21 Subclass.

22 183. T-Mobile advertised, offered, or sold goods or services in North Carolina and
23 engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as
24 defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

1 184. T-Mobile engaged in unfair and deceptive acts and practices in or affecting
2 commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

3 a. Failing to implement and maintain reasonable security and privacy measures to
4 protect Plaintiff Miller and North Carolina Subclass members' Private Information,
5 which was a direct and proximate cause of the Data Breach;

6 b. Failing to identify foreseeable security and privacy risks, remediate identified
7 security and privacy risks, and adequately improve security and privacy measures
8 following previous cybersecurity incidents, which was a direct and proximate cause
9 of the Data Breach;

10 c. Failing to comply with common law and statutory duties pertaining to the security
11 and privacy of Plaintiff Miller's and North Carolina Subclass members' Private
12 Information.

13 185. T-Mobile's representations and omissions were material because they were likely
14 to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to
15 protect the confidentiality of consumers' Private Information.

16 186. T-Mobile intended to mislead Plaintiff Miller and North Carolina Subclass
17 members and induce them to rely on its misrepresentations and omissions.

18 187. Had T-Mobile disclosed to Plaintiff Miller and North Carolina Subclass members
19 that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been
20 unable to continue in business and it would have been forced to adopt reasonable data security
21 measures and comply with the law. T-Mobile was trusted with sensitive and valuable Private
22 Information regarding millions of consumers, including Plaintiff Miller and the North Carolina
23 Subclass. Plaintiff Miller and the North Carolina Subclass members acted reasonably in relying
24

1 on T-Mobile's misrepresentations and omissions, the truth of which they could not have
2 discovered.

3 188. T-Mobile acted intentionally, knowingly, and maliciously to violate North
4 Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff Miller's and North
5 Carolina Subclass members' rights. T-Mobile's numerous past data breaches put it on notice that
6 its security and privacy protections were inadequate.

7 189. As a direct and proximate result of T-Mobile's unfair and deceptive acts and
8 practices, Plaintiff Miller and North Carolina Subclass members have been harmed and have
9 suffered damages including, but not limited to: damages arising from identity theft and fraud;
10 out-of-pocket expenses associated with procuring identity protection and restoration services;
11 increased risk of future identity theft and fraud, and the costs associated therewith; and time spent
12 monitoring, addressing and correcting the current and future consequences of the Data Breach.

13 190. Plaintiff Miller and North Carolina Subclass members seek all monetary and non-
14 monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees
15 and costs.

16 **COUNT XII**
17 **VIOLATION OF DECEPTIVE TRADE PRACTICES – CONSUMER**
18 **PROTECTION ACT, Texas Bus. & Com. Code §§ 17.41, *et seq.***
19 **(On Behalf of the Texas Subclass)**

20 191. Plaintiffs re-allege and incorporate by reference herein all the allegations
21 contained above.

22 192. Plaintiff Karla Williams asserts this claim on behalf of the Texas Subclass.

23 193. T-Mobile is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

24 194. Plaintiff Williams and the Texas Subclass members are "consumers," as defined
by Tex. Bus. & Com. Code § 17.45(4).

1 195. T-Mobile advertised, offered, or sold goods or services in Texas and engaged in
 2 trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus.
 3 & Com. Code § 17.45(6).

4 196. T-Mobile engaged in false, misleading, or deceptive acts and practices, in
 5 violation of Tex. Bus. & Com. Code § 17.46(b), including:

- 6 a. Representing that goods or services have sponsorship, approval, characteristics,
 7 ingredients, uses, benefits, or quantities that they do not have;
- 8 b. Representing that goods or services are of a particular standard, quality or grade,
 9 if they are of another; and
- 10 c. Advertising goods or services with intent not to sell them as advertised.

11 197. T-Mobile's false, misleading, and deceptive acts and practices include:

- 12 a. Failing to implement and maintain reasonable security and privacy measures to
 13 protect Plaintiff Williams's and Texas Subclass members' Private Information,
 14 which was a direct and proximate cause of the Data Breach;
- 15 b. Failing to identify foreseeable security and privacy risks, remediate identified
 16 security and privacy risks, and adequately improve security and privacy measures
 17 following previous cybersecurity incidents, which was a direct and proximate
 18 cause of the Data Breach; and
- 19 c. Failing to comply with common law and statutory duties pertaining to the security
 20 and privacy of Plaintiff Williams's and Texas Subclass members' Private
 21 Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and
 22 Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a
 23 direct and proximate cause of the Data Breach;

1 198. T-Mobile intended to mislead Plaintiff Williams and Texas Subclass members
2 and induce them to rely on its misrepresentations and omissions.

3 199. T-Mobile's representations and omissions were material because they were likely
4 to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to
5 protect the confidentiality of consumers' Private Information.

6 200. Had T-Mobile disclosed to Plaintiff Williams and Texas Subclass members that
7 its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable
8 to continue in business and it would have been forced to adopt reasonable data security measures
9 and comply with the law. Because T-Mobile held itself out as being capable of protecting and
10 maintaining the Private Information entrusted to it by consumers, including Plaintiff Williams
11 and the Texas Subclass, Plaintiff Williams and the Texas Subclass members acted reasonably in
12 relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have
13 discovered.

14 201. T-Mobile had a duty to disclose the above facts due to the sensitivity and of the
15 Private Information in its possession, and the industry standards for the protection of critical
16 Private Information. This duty arises because consumers, including Plaintiff Williams and the
17 members of the Texas Subclass are required to entrust their sensitive Private Information to T-
18 Mobile in order to receive wireless services from T-Mobile.

19 202. T-Mobile engaged in unconscionable actions or courses of conduct, in violation
20 of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). T-Mobile engaged in acts or practices which, to
21 consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or
22 capacity to a grossly unfair degree.

23 203. Consumers, including Plaintiff Williams and Texas Subclass members, lacked
24

1 knowledge about deficiencies in T-Mobile's data security because this information was known
2 exclusively by T-Mobile. Consumers also lacked the ability, experience, or capacity to secure
3 the Private Information in T-Mobile's possession or to fully protect their interests with regard to
4 their data. Plaintiff and Texas Subclass members lack expertise in information security matters
5 and do not have access to T-Mobile's systems in order to evaluate its security controls. T-Mobile
6 took advantage of its special skill and access to Private Information to hide its inability to protect
7 the security and confidentiality of Plaintiff Williams's and Texas Subclass members' Private
8 Information.

9 204. T-Mobile intended to take advantage of consumers' lack of knowledge, ability,
10 experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that
11 would result.

12 205. T-Mobile acted intentionally, knowingly, and maliciously to violate Texas's
13 Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff
14 Williams's and Texas Subclass members' rights. T-Mobile's numerous past data breaches put it
15 on notice that its security and privacy protections were inadequate.

16 206. As a direct and proximate result of T-Mobile's unlawful practices and acts,
17 Plaintiff Williams and Texas Subclass members have been harmed and have suffered damages
18 including, but not limited to: damages arising from identity theft and fraud; out-of-pocket
19 expenses associated with procuring identity protection and restoration services; increased risk of
20 future identity theft and fraud, and the costs associated therewith; and time spent monitoring,
21 addressing and correcting the current and future consequences of the Data Breach.

22 207. T-Mobile's violations present a continuing risk to Plaintiff Williams and Texas
23 Subclass members as well as to the general public.

208. If T-Mobile fails to provide appropriate relief for its violations of the Deceptive Trade Practices Act, Plaintiff Williams will amend this complaint accordingly to seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

COUNT XIII
VIOLATION OF WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT,
W. Va. Code §§ 46A-6-101, *et seq.*
 (On behalf of the West Virginia Subclass)

209. Plaintiffs re-allege and incorporate by reference herein all the allegations contained above.

210. Plaintiff Chris Jarvis asserts this claim on behalf of the West Virginia Subclass.

211. Plaintiff Jarvis and West Virginia Subclass members are "consumers," as defined by W. Va. Code § 46A-6-102(2).

212. T-Mobile engaged in "consumer transactions," as defined by W. Va. Code § 46A-6-102(2).

213. T-Mobile advertised, offered, or sold goods or services in West Virginia and engaged in trade or commerce directly or indirectly affecting the people of West Virginia, as defined by W. Va. Code § 46A-6-102(6).

214. T-Mobile engaged in unfair and deceptive business acts and practices in the conduct of trade or commerce, in violation of W. Va. Code § 46A-6-104, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Jarvis and West Virginia Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

1 b. Failing to identify foreseeable security and privacy risks, remediate identified
2 security and privacy risks, and adequately improve security and privacy measures
3 following previous cybersecurity incidents, which was a direct and proximate cause
4 of the Data Breach; and

5 c. Failing to comply with common law and statutory duties pertaining to the security
6 and privacy of Plaintiff Jarvis and West Virginia Subclass members' Private
7 Information.

8 215. T-Mobile's unfair and deceptive acts and practices were unreasonable when
9 weighed against the need to develop or preserve business, and were injurious to the public
10 interest, under W. Va. Code § 46A-6-101.

11 216. T-Mobile's acts and practices were additionally "unfair" under W. Va. Code §
12 46A-6-104 because they caused, or were likely to cause, substantial injury to consumers which
13 was not reasonably avoidable by consumers themselves and not outweighed by countervailing
14 benefits to consumers or to competition.

15 217. The injury to consumers from T-Mobile's conduct was, and is, substantial because
16 it was non-trivial and non-speculative. The injury to consumers was substantial not only because
17 it inflicted harm on a significant and unprecedented number of consumers, but also because it
18 inflicted a significant amount of harm on each consumer.

19 218. Consumers could not have reasonably avoided injury because T-Mobile's
20 business acts and practices unreasonably created or took advantage of an obstacle to the free
21 exercise of consumer decision-making. By withholding important information from consumers
22 about the inadequacy of its data security, T-Mobile created an asymmetry of information between
23 it and consumers that precluded consumers from taking action to avoid or mitigate injury.
24

1 219. T-Mobile's inadequate data security had no countervailing benefit to consumers
2 or to competition.

3 220. T-Mobile's acts and practices were additionally "deceptive" under W. Va. Code
4 § 46A-6-104 because T-Mobile made representations or omissions of material facts that misled
5 or were likely to mislead reasonable consumers, including Plaintiff Jarvis and West Virginia
6 Subclass members.

7 221. T-Mobile intended to mislead Plaintiff Jarvis and West Virginia Subclass
8 members and induce them to rely on its misrepresentations and omissions.

9 222. T-Mobile's representations and omissions were material because they were likely
10 to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to
11 protect the confidentiality of consumers' Private Information.

12 223. Had T-Mobile disclosed to Plaintiff Jarvis and Class members that its data
13 systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to
14 continue in business and it would have been forced to adopt reasonable data security measures
15 and comply with the law. T-Mobile was trusted with sensitive and valuable Private Information
16 regarding millions of consumers, including Plaintiff Jarvis and the West Virginia Subclass.
17 Plaintiff Jarvis and the West Virginia Subclass members acted reasonably in relying on T-
18 Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

19 224. T-Mobile acted intentionally, knowingly, and maliciously to violate West
20 Virginia's Consumer Credit and Protection Act, and recklessly disregarded Plaintiff Jarvis and
21 West Virginia Subclass members' rights. T-Mobile's unfair and deceptive acts and practices were
22 likely to cause serious harm. T-Mobile's numerous past data breaches put it on notice that its
23 security and privacy protections were inadequate.

225. As a direct and proximate result of T-Mobile's unfair and deceptive acts or practices and Plaintiff Jarvis and West Virginia Subclass members' purchase of goods or services, Plaintiff Jarvis and West Virginia Subclass members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

226. Plaintiff Jarvis and West Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$200 per violation under W. Va. Code § 46A-6-106(a), restitution, injunctive and other equitable relief, punitive damages, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and on behalf of the Class, respectfully requests that this Court enter an Order:

- a) Certifying the proposed Class, and appointing Plaintiffs as Class Representatives;
- b) Finding that T-Mobile's conduct was negligent, deceptive, unfair, and unlawful as alleged herein;
- c) Enjoining T-Mobile from engaging in further negligent, deceptive, unfair, and unlawful business practices as alleged herein;
- d) Awarding Plaintiffs and Class members actual, compensatory, and consequential damages;
- e) Awarding Plaintiffs and Class members statutory damages and penalties, as allowed by law;

- 1 f) Awarding Plaintiffs and Class members pre-judgment and post-judgment interest;
2 g) Awarding Plaintiffs and Class members reasonable attorneys' fees, costs, and
3 expenses; and
4 h) Granting such other relief as the Court deems just and proper.

5 **DEMAND FOR JURY TRIAL**

6 Plaintiffs, on behalf of themselves and the proposed Classes, hereby demand a trial by
7 jury as to all matters so triable.

8 DATED: September 13, 2021

9 TOUSLEY BRAIN STEPHENS PLLC

10 s/ Kim D. Stephens

Kim D. Stephens, WSBA #11984
kstephens@tousley.com

11 s/ Jason T. Dennett

Jason T. Dennett, WSBA #30686
jdennett@tousley.com

12 s/ Kaleigh N. Powell

Kaleigh N. Powell, WSBA #52684
kpowell@tousley.com

13 1200 Fifth Avenue, Suite 1700
14 Seattle, WA 98101

Ph: (206) 682-5600; Fax (206) 682-2992

15 **LEVI & KORSINSKY, LLP**

16 Mark S. Reich (*pro hac vice* to be filed)
17 Courtney E. Maccarone (*pro hac vice* to be filed)

55 Broadway, 10th Floor

New York, NY 10006

18 Tel: (212) 363-7500

mreich@zlk.com

19 cmaccarone@zlk.com

20 *Attorneys for Plaintiffs and Proposed Class*